PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06K 7/08, 7/10

A1

(11) International Publication Number: WO 97/01826

(43) International Publication Date: 16 January 1997 (16.01.97)

(21) International Application Number: PCT/GB96/01535

(22) International Filing Date: 26 June 1996 (26.06.96)

(30) Priority Data:
9512953.2 26 June 1995 (26.06.95) GB

(71) Applicant *(for all designated States except US)*: MEDESTATE LTD. [BS/BS]; Cumberland House, 27 Cumberland Street, P.O. Box N8308, Nassau (BS).

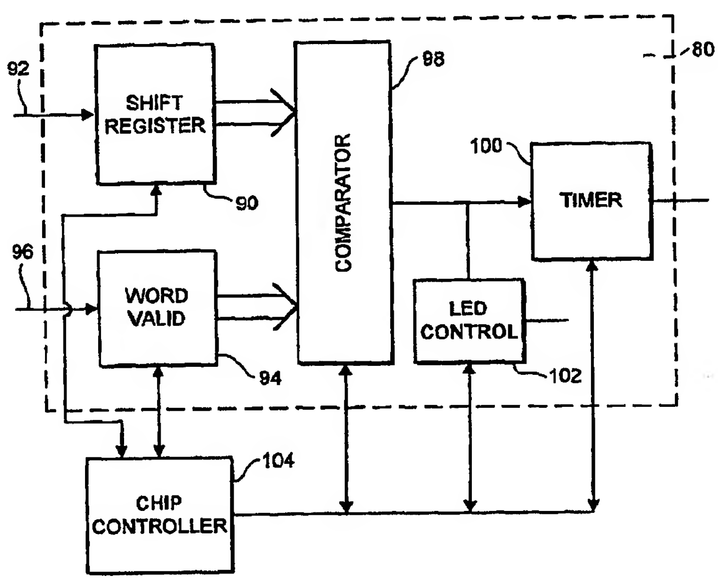
(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: MITCHESON, Mark [GB/GB]; Cemetery Park Lodge House, Loftus, Cleveland TS13 4LZ (GB). HADDAWAY, Kevin [GB/GB]; TagSystems Limited, St. Cuthberts House, St. Cuthberts Way, Newton Aycliffe, Co. Durham DL5 6AW (GB).

(74) Agents: DRIVER, Virginia, Rozanne et al.; Page White & Farrer, 54 Doughty Street, London WC1N 2LS (GB).

(81) Designated States: GB, JP, US, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: TAG DETECTION SYSTEM



(57) Abstract

A way of monitoring tags within a monitored volume is disclosed. A plurality of tags each has a store holding a unique identification comprising a first level code and a second level code. Each tag also has a comparator for selectively comparing incoming codes with one of the first level code and the second level code. A tag detector transmits a plurality of codes in sequence to uniquely identify one of the tags. The tag detector transmits a first level code and only transmits a second level code if at least one of the tags with a first level code matching the transmitted first level code has responded. The provision of first and second level codes allows the length of each code to be reduced and still allow a large tag population.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia	**GB**	United Kingdom	**MW**	Malawi
AT	Austria	**GE**	Georgia	**MX**	Mexico
AU	Australia	**GN**	Guinea	**NE**	Niger
BB	Barbados	**GR**	Greece	**NL**	Netherlands
BE	Belgium	**HU**	Hungary	**NO**	Norway
BF	Burkina Faso	**IE**	Ireland	**NZ**	New Zealand
BG	Bulgaria	**IT**	Italy	**PL**	Poland
BJ	Benin	**JP**	Japan	**PT**	Portugal
BR	Brazil	**KE**	Kenya	**RO**	Romania
BY	Belarus	**KG**	Kyrgystan	**RU**	Russian Federation
CA	Canada	**KP**	Democratic People's Republic of Korea	**SD**	Sudan
CF	Central African Republic			**SE**	Sweden
CG	Congo	**KR**	Republic of Korea	**SG**	Singapore
CH	Switzerland	**KZ**	Kazakhstan	**SI**	Slovenia
CI	Côte d'Ivoire	**LI**	Liechtenstein	**SK**	Slovakia
CM	Cameroon	**LK**	Sri Lanka	**SN**	Senegal
CN	China	**LR**	Liberia	**SZ**	Swaziland
CS	Czechoslovakia	**LT**	Lithuania	**TD**	Chad
CZ	Czech Republic	**LU**	Luxembourg	**TG**	Togo
DE	Germany	**LV**	Latvia	**TJ**	Tajikistan
DK	Denmark	**MC**	Monaco	**TT**	Trinidad and Tobago
EE	Estonia	**MD**	Republic of Moldova	**UA**	Ukraine
ES	Spain	**MG**	Madagascar	**UG**	Uganda
FI	Finland	**ML**	Mali	**US**	United States of America
FR	France	**MN**	Mongolia	**UZ**	Uzbekistan
GA	Gabon	**MR**	Mauritania	**VN**	Viet Nam

Title of the Invention

TAG DETECTION SYSTEM

Field of the Invention

The present invention relates to a tag detection system.

The tag detection system is particularly appropriate for use with a tag monitoring system and a tag described in our Patent Application filed on 21st June 1996 entitled "A Tag and Tag Monitoring System" (Page White & Farrer Reference 81971) the contents of which are herein incorporated by reference.

Background of the Invention

One way of monitoring tags is to transmit a signal which includes a message which triggers all of the tags within a monitored volume. Any tags within the monitored volume then issue a response which identifies each tag uniquely. When a plurality of tags are present within the monitored volume, they must issue responses in a way which prevents them from interfering with one another, i.e. on different time slots or on different fequencies. This requires the use of complex detection electronics at the tag detector.

As an alternative, the transmitted signal can consist of a series of codes, each code uniquely identifying a tag. Each tag has stored within it a unique code which is compared at the tag with the transmitted code. When the transmitted code matches the code stored within a tag, only that tag will respond.

The latter technique has a significant advantage that the responses from the tags can all be the same. However, a large number of different codes is required to uniquely identify tags, and this places practical limitations on the number of tags that can be used within the detection system.

Summary of the Invention

According to the present invention there is provided a tag detection system comprising:

a plurality of tags each having a store holding a unique identification comprising a first level code and a second level code and a comparator for selectively comparing incoming codes with one of said first level code and second level code; and

a tag detector operable to transmit in sequence a plurality of codes to uniquely identify one of said tags, the tag detector being arranged to transmit a first level code and, only if at least one of said plurality of tags has a first level code matching the transmitted first level code, to issue a second level code.

By providing first level codes and second level codes, the length of each code can be reduced and still provide a large tag population.

Preferably, each tag includes a receiver for receiving electromagnetic signals and wherein the tag detector transmits said sequence of codes using electromagnetic signals.

Each tag preferably comprises circuitry for issuing a response when a first level code transmitted by the tag detector matches the first level code held in the tag.

In the preferred embodiment, each tag has a flag which is set when a first level code has been received by the tag which does not match its stored first level code, to inhibit responses to subsequently transmitted second level codes.

The invention is not restricted to the use only of first level codes and second level codes. There may be any number of different levels according to the requirements of the system.

The invention also provides a tag for use in a tag detection system as defined hereinabove which comprises:

a store holding a unique identification comprising a first level code and a second level code;

a receiver for receiving a sequence of incoming codes;

a comparator for comparing each of said incoming codes selectively with one of said first level code and second level code held in the store; and

a response controlling circuit for issuing a response when an incoming code matches the first level code or second level code held in the store.

The invention also provides a method of uniquely identifying one of a plurality of tags, each tag having a unique identification comprising a first level code and a second level code and means for issuing a response if an incoming code selectively matches one of said first level code and second level code, the method comprising:

issuing a first level code and awaiting any responses from tags, and, in the event that a response is received issuing a second level code and awaiting responses and, in the event that no response is received, issuing a next first level code and awaiting responses.

For a better understanding of the present invention and to show how the same may be carried into effect reference will now be made by way of example to the accompanying drawings.

Brief Description of the Drawings

Figure 1 is a block diagram of a tag monitoring system;

Figure 1a is a diagram of a gate zone;

Figure 2 illustrates how a domain is defined using beacon sets;

Figure 3 is a diagram representing how the beacon sets are activated in each domain;

Figure 4 is a block diagram of elements of a domain controller;

Figure 5 is a diagrammatic sketch indicating operation of the domain controller;

Figure 6 is a block diagram of the main components of a tag for use in the system;

Figure 7 is a block diagram of logic circuitry of the tag;

Figures 8 and 9 represent bit sequences respectively of the upper level code and lower level code.

Description of the Preferred Embodiment

Figure 1 is a block diagram of a tag monitoring system. Reference numeral 2 denotes a communication network by means of which the components of the monitoring system are able to communicate. The monitoring system comprises a tag issue unit 4 connected to a tag reader 6. The tag issue unit 4 is connected to the network 2. Also forming part of the monitoring system are first and second domain controllers 10,12 which are each connected to the network 2. There is also a data concentrater 14 connected to the network 2 and four gate controllers 16,18,20,22 each connected to the network 2. It will be appreciated from the following description that the number of domain controllers and gate controllers can be selected according to the requirements of the monitoring system. Each gate controller defines two zones indicated in Figure 1 as zone A and zone B. Those zones are separated by a physical boundary. These are illustrated only for the gate controller 22 but will be defined for each of the gate controllers 16,18 and 20. The first domain controller 10 is in communication with five domains labelled Domain A to Domain E respectively. The second domain controller 12 is connected to three domains labelled Domain F to Domain H. These domains are not defined by physical boundaries but by a scanning system described in more detail hereinafter.

Tags are issued at the tag issue unit 4. Each tag includes a receiver and transmitter for respectively receiving and transmitting radio frequency (RF) signals allowing the tag to communicate with the monitoring system.

An overall volume to be monitored is defined by a physical boundary. That boundary has a set of exits/entrances, each of which is monitored by a gate controller. Each gate controller has two separate sets of antennas, one monitoring zone A, for example inside the volume, and the other monitoring zone B, outside the volume.

Figure 1a is a diagram in the region of such an exit/entrance. Reference numeral 1 denotes the wall constituting the physical boundary defining the exit/entrance 3.

Each of the domains A to H is a sub-volume within the main volume in which tags may be detected. The domains are within the physical boundary. The domains are defined by tag detection antennae (beacons) distributed throughout the volume. The beacons are arranged in a plurality of beacon sets, with each set comprising a plurality of beacons connected to be activated together. Depending on the size and nature of the domain to be defined, any number of beacon sets can be utilised. The beacon sets are arranged so that there is full coverage throughout the domain volume. Figure 2 shows a domain having two beacon sets. The first beacon set BEACON SET 1 is shown shaded on the left hand side of Figure 2 and comprises five beacons whose area of coverage is illustrated diagrammatically by the outer circumferences of the circles. Reference numeral 24 denotes a beacon. The diagram on the right hand side of Figure 2 represents the second beacon set BEACON SET 2 having four beacons arranged at different locations to give a different radar coverage to that given by BEACON SET 1.

The monitoring system is arranged so that it is possible to detect the location of tags within the volume covered by the monitoring system. To this end, each gate zone and domain is polled to determine whether or not tags are in the zone or domain respectively.

For the purposes of polling each domain, each domain controller has transmit and receive beacon set controlling switches 26,28 illustrated diagrammatically in Figure 3. There is a set of such switches for each domain to be polled by the domain controller. The transmit switch 26 has four terminals T1 to T4 and the receive switch has four terminals R1 to R4. Each beacon 24 consists of a transmit antenna A_t and a receive antenna A_r. The transmit antennas A_t of BEACON SET 1 are connected to the first terminal T1 of the transmit switch 26. The receive antennas A_r of the BEACON SET 1 are connected to terminal R1 of the receive switch 28. Similarly, the transmit antennas of BEACON SET 2 are connected to the second terminal T2 of the transmit switch 26, and transmit antennas of subsequent beacon sets are connected to the remaining terminals T3,T4. Likewise, the receive antennas of BEACON SET 2 are connected to the second terminal R2 of the receive switch 28. The receive antennas of subsequent beacon sets are connected to the remaining receive terminals R3,R4. In operation, transmit switch 26 is firstly connected to the first terminal T1 and the receive switch 28 is connected to its first terminal R1. A signal is transmitted through the transmit antennas A_t of the first beacon set 1 and any signals received are supplied to the receive switch 28 from the receive antennas. The transmit signal is denoted T_x and the received signal is denoted R_x. Then, the transmit and receive switches 26,28 are connected to the second terminals T2,R2 and the process of transmitting a signal T_x and waiting for any receive signal R_x is repeated. Once all beacon sets within a domain have been activated, the transmit

and receive switches return to the first terminal to begin the sequence again.

As explained above, each domain controller has a plurality of sets of transmit and receive switches 26,28, there being one set for each domain to be polled by the domain controller. Figure 4 is a block diagram of the main components of each domain controller. The sets of transmit and receive switches are contained within a router 30. The router 30 has a plurality of ports (five in the case of domain controller 10 and three in the case of domain controller 12). These ports are denoted in Figure 4 as P1 to P5. Each port is bidirectional and is capable of receiving and transmitting signals between the domains and the domain controller. The router 30 is connected via a two-way communication path to an interface 32. The interface itself communicates with a microprocessor 34. The microprocessor 34 is also connected to the network 2 via a two-way communication path 36. The microprocessor 34 controls polling of the domains by the domain controller.

Figure 5 is a diagram for the purposes of explaining how the microprocessor 34 operates to control polling of domains. It will be appreciated that Figure 5 is diagrammatic only and that the processes and databases illustrated in Figure 5 may be organised in any appropriate manner within the microprocessor 34. There are a set of poll databases 40 each holding up-to-date information concerning the locations of tags issued by the tag issue unit 4. There is a poll database for each domain controlled by the domain controller. Each poll database 40 holds information concerning tag IDs, the location of the tags, the time and date. When a tag is first issued by the tag issue unit, its identity is read by the tag reader 6, the system is set to mark the tag as active and its location is set to a default location, e.g. INSIDE. A tag detection process updates the poll databases as each domain is

polled. The tag detection process 42 causes the microprocessor to output signals to the router 30 to control connection of the transmit and receive switches 26,28 and generates the signals T_x to be transmitted. These signals are referred to herein as interrogation signals. The interrogation signals interrogate the domain which is currently being polled and any responses received from that domain are supplied (via the router 30 and interface 32) to the tag detection process. The interrogation signals which are supplied during polling of each domain allow tags within that domain to be identified. The poll database for each domain is continuously updated during polling of that domain. A time process 44 receives data from the poll database for the domain being polled and ascertains the following:

1) has the same tag been detected x times in y seconds? (if yes, assume tag entered domain);
2) same tag not detected x times in y seconds? (if yes, assume tag left domain).

The results of the time process 44 are used to update a plurality of valid detect databases 46, one database for each domain. The valid detect databases hold for each tag, the tag ID, its location, the time and date. Against each entry, a flag is set to indicate whether or not there has been a movement of that tag since the last time the database was updated. Information concerning movements of tags is supplied to the data concentrater 14 via a data concentrater communication process 48. When a request is made by the data concentrater for information, the data concentrater communication process accesses the valid detect databases 46 and supplies the information concerning any flagged movements to the data concentrater.

When tags are issued at the tag issue unit 4, information is supplied to the data concentrater via the network 2 concerning

the tag ID and the expiry time of that tag. That is, when the tags are used to monitor the movements of persons who have paid to enter an activity centre or the like, it is desirable to allow these persons access only for a predetermined period of time. The time after which they no longer are permitted to remain in the activity centre is entered as the expiry time. The tag IDs and expiry times are held in an expiry database 50 within the domain controller. When the expiry time of a particular tag has been reached, the identity of that tag is supplied to the tag detection process 42 which issues an appropriate signal to the router to control subsequent transmitted signals for that tag.

Figure 6 is a block diagram illustrating the main components of a tag. Each tag can take the form of a watch type device to be worn on the wrist of a wearer and has its own battery. Batteryless tags may also be possible, activated via received signals. The tag comprises an RF receiver 70 for receiving transmitted signals T_x from the domain controller or gate controller. A diode detector 72 is connected to the RF receiver 70. Transistor circuitry 74 in the form of an emitter follower and common emitter prepare the received RF signal for supply to a tag chip 76. The tag chip 76 includes an A/D converter 78 which receives the analogue signal from the transistor circuitry 74 and supplies a corresponding digital signal to logic circuitry 80. The logic circuitry 80 controls a transmit antenna 82 to transmit a suitable response signal R_x from the tag. The tag additionally comprises a light emitting diode (LED) 84 connected to the output of the logic circuitry 80 via a resistor 86. The purpose of this light emitting diode is to provide a visual indication at each tag. The light emitting diode 84 can be activated from the domain controller by including an appropriate message in the signal T_x transmitted from the domain controller. In one application, a signal is transmitted to a tag when the valid

time on the tag has expired, as stored in the expiry database 50 of the domain controller. Thus, the light emitting diode will light up when the valid time for that tag has expired, thereby indicating to a supervisor that that person should be removed from the monitored area.

It is also possible to use the light emitting diode in emergency situations by causing a signal to be transmitted to all tags including a message to activate the light emitting diode on each tag to render the wearers of the tags more visible to fire personnel or the like.

Figure 7 is a block diagram showing details of the logic circuitry 80. The logic circuitry 80 includes a shift register 90 which is an eleven bit shift register. This holds a unique identification code for the tag in the form of a six bit word constituting an upper level code and a five bit word constituting a lower level code. The shift register has an input 92 allowing the identification code of the tag to be entered. The logic circuitry 80 includes a word valid circuit 94 which is a shift register for holding data from the A to D converter 78 derived from incoming signals T_x from the domain controller. The input line to the word valid circuit 94 is denoted by reference numeral 96. Outputs from the shift register 90 and word valid circuit 94 are supplied to a comparator 98 in a manner described in more detail hereinafter. The output of the comparator controls a timer 100 which in turn controls the transmit antenna 82. The output of the comparator 98 is also supplied to an LED control circuit 102 which controls the LED 84.

The tag chip 76 includes a chip controller 104 for managing the logic circuitry 80.

Polling of the domains will now be described in more detail. When a tag is issued at the tag issue unit 4, the identity of

the tag is read by the tag reader 6 and the tag ID is supplied to the data concentrater 14 together with the date and time and default location. At any time, there will be a large number of tags within the monitored volume, and the aim of the present monitoring system is to keep track of the location of those tags within the monitored volume. To poll domain A, the domain controller 10 sets the transmit and receive switches 26,28 of the first port P1 (which is connected to domain A). The transmit and receive switches 26,28 are connected to their first terminals T1,R1 to activate BEACON SET 1 within domain A. A first bit sequence is transmitted via the transmit antennas A_t of BEACON SET 1. The first bit sequence is illustrated in Figure 8 marked ULCS (upper level code sequence). The bit sequence includes a start bit 50, a parity bit 52, a level descripter 54, six bits of data defining the upper level code ULC and finally a stop bit 55. The transmission time for that bit sequence is of the order of 104u. That sequence is received by all tags within the domain and the data bits of the upper level code are compared with the stored ULC within each tag. The domain controller has a wait period of less than 500u within which to receive responses from tags in that domain. Any tag in that domain for which its ULC matches the transmitted ULC issues a response signal. The response signal from all tags is the same. The timer 100 modulates the transmitted signal with nine cycles of 48kHz. If no response is received, a next ULC bit sequence is transmitted with a different set of six data bits representing the ULC. If there is at least one response, a lower level code bit sequence is transmitted. This is illustrated in Figure 9 marked LLCS. In the lower level code bit sequence there is a start bit 60, a parity bit 62, a level descripter 64, five bits of LLC data, an expiry bit 66 and a stop bit 67. If the transmitted ULC does not match the stored ULC of a tag, a flag is set in the chip controller 104 so that those tags will not respond to subsequent lower level codes.

At each with a ULC matching the previously transmitted ULC tag the data bits in the lower level code are compared with the stored LLC and the domain controller waits for a response. If there is no response, it sends out a next lower level code bit sequence. If a response is received, a tag in that domain has been uniquely identified by the combination of upper level code and lower level code and the identity of this tag and its location is entered into the poll database 40 associated with domain A. Moreover, the expiry bit for that tag is examined at the tag to see whether the LED is to be activated.

The same bit sequences are transmitted x number of times to allow the time process 44 to determine whether or not a valid detection has been made. When this sequence of events has been carried out with the transmit and receive switches 26,28 connected to their first terminal T1,R1, they are switched over to their second terminals T2,R2 and the sequence of events is repeated again in precisely the same manner. When the number of switch terminals corresponding to the number of beacon sets in that domain have all been used, polling returns to the first terminals. The domain controller can poll all of the domains simultaneously. Thus, it is capable of controlling transmit signals T_x for transmission to each of the domains for which it is responsible. It will readily be apparent that it may be transmitting different code sequences from different ports, depending on the responses that have been received from different domains.

It is convenient if the upper level code sequences are transmitted in numerical order, being decremented by one between each transmission. Likewise, the lower level code sequences can similarly be decremented by one before each transmission.

The gates can be polled in a similar fashion. While a tag remains within zone A (i.e. the wearer does not pass through

the exit/entrance zone 3 into zone B), no change is made to the data stored at the data concentrater concerning the location of that tag. The data concentrater will already hold information for that tag concerning the domain inside the physical boundary within which the tag is located. If however a tag is detected in zone B, the gate controller will immediately notify the data concentrater via the network 2 to indicate that a wearer is now outside the physical boundary.

The data concentrater 14 thus holds up-to-date information concerning the identity of each tag which has been issued at the tag issue unit with the location of that tag. This information can be accessed by a file server 8 attached to the network 2 and displayed. This means that in the event of an emergency, the location of each person within the monitored volume is known. This assists fire officers and safety personnel in their rescue attempts. Moreover, if there is an emergency evacuation, it is possible to detect, using the gate controllers, that the holders of all issued tags have left the building.

Thus in the above described polling system, the tag stores two sequences of bits (an upper level code (ULC) and a lower level code (LLC)). The ULC has m bits where m=6. The domain controller transmits 2^m codes, with the level descripter bit 54 set to identify the code sequences as upper level codes. When one or more tags reply to this code both the domain controller and the tags move down to the lower level of interrogation.

The gate now transmits the lower level sequence of codes with the level descripter bit 64 reset to identify that the interrogation is being carried out at the lower level. Only one tag will respond to a given lower level code. Tags will share upper level codes and lower level codes, though no two

tags will have the same upper and lower level code. Hence any tag can be uniquely identified.

Although two levels are described herein, there is no theoretical limit to the number of levels and the number of bits per level.

In a system where the tags have n levels, with the same number (m) of bits per level, then the characteristics of the polling technique for that system are;

number of codes per level:	2^m
maximum tag population:	$2^{(m \times n)}$
number of transmissions T_x:	$n \times (2^m)$
number of stored bits:	$m \times n$
number of bits for n levels:	$\log_2 n$
total number of T_x bits:	$m + \log_2 n$

From these equations it is not immediately obvious how the interrogation rate varies with the tag population, number of levels and number of bits per level. Table I illustrates these variations for a system based around 6 transmitted bits:

BITS PER LEVEL m	NO. OF LEVELS n	NO. OF CODES $2^{(m \times n)}$	NO. OF STORED BITS $m \times n$	NO. OF GATE TRANSMISSIONS 2^6
6	1	64	6	64
5	2	1024	10	64
4	4	65,536	16	64
3	8	16,777,216	24	64
2	16	4,294,967,296	32	64
1	32	4,294,967,296	32	64

<u>Tag Populations and Interrogation Cycles</u>

<u>Table I</u>

Table I illustrates the following points:

(a) The maximum number of transmissions needed to locate a specific tag is constant with the transmitted gate word size.

(b) As the number of levels increase, the number of bits stored in the tag increases (also the number of tag replies increases).

(c) The maximum tag population rises in an exponential manner as the number of levels increases.

It should be apparent that choosing a specific interrocation technique is a compromise between the maximum tag population,

the number of tag replies, location speed and tag and software complexity.

The domain controller continually counts down through ULCs, pausing after each transmission to "listen" for a tag response. When a reply is detected, the domain controller re-transmits that ULC to confirm that the tag has replied. This verification of a tag's presence is the basis of the error detection capabilities of the system.

Once a ULC has been verified both the domain controller and the tag will move down to the lower level (the chip controller 102 of the tag keeps a count of how many replies it has made during an interrogation sequence). If several tags have replied to the same ULC then they will have difference LLCs and will be identified as individuals during this next stage of interrogation. No tags will reply to a LLC if they have not been verified at the upper level.

The domain controller then counts down through the LLCs until a tag is detected. As previously described this code will be re-transmitted to verify the tag's presence. This tag has now been completely detected and verified. Counting down continues through the LLCs until all tags that have moved down an interrogation level are verified.

Once all lower level tags have been verified then the ULC countdown continues at the next lower code to that where the jump into the LLCs occurred.

There are several stages of error trapping inherent in the design of the system, as detailed below.

(a) The verification of detected replies.

(b) The tags will only reply to a valid word with a matching ULC or LLC.

(c) A tag will only reply to correct codes on the correct level.

(d) If an upper level verify is missed and the tag moves down a level then a tag will reset to the upper level as soon as it detects that an upper level code is being transmitted.

(e) If a lower level verify is missed and the tag switches off then a special procedure will reset all tags in the domain.

This system is very reliable and in tests no tags were detected due to a tag replying to a gate transmit sequence that it was not meant to reply to.

The tag monitoring system described herein has applications in many different areas where it is required to monitor the locations of persons within a site or building, e.g. workers in hazardous environments, babies in hospitals, security and access control systems.

CLAIMS:

1. A tag detection system comprising:

a plurality of tags each having a store holding a unique identification comprising a first level code and a second level code and a comparator for selectively comparing incoming codes with one of said first level code and second level code; and

a tag detector operable to transmit in sequence a plurality of codes to uniquely identify one of said tags, the tag detector being arranged to transmit a first level code and, only if at least one of said plurality of tags has a first level code matching the transmitted first level code, to issue a second level code.

2. A tag detection system according to claim 1 wherein each of the plurality of tags includes a receiver for receiving electromagnetic signals and wherein the tag detector transmits said sequence of codes using electromagnetic signals.

3. A tag detection system according to claim 1 or 2 wherein each tag comprises circuitry for issuing a response when a first level code transmitted by the tag detector matches the first level code held in the tag.

4. A tag detection system according to any preceding claim wherein each tag comprises a flag which is set when a first level code has been received by the tag which does not match its stored first level code, to inhibit responses to subsequently transmitted second level codes.

5. A tag detection system according to any preceding claim wherein there is at least one further level code held in each tag and transmitted in the sequences transmitted by the tag detector.

6. A tag detection system according to any preceding claim wherein the tag detector transmits the same first level code a plurality of times before transmitting a different first level code or a second level code to validate detection.

7. A tag for use in a tag detection system according to any preceding claim which comprises:

a store holding a unique identification comprising a first level code and a second level code;

a receiver for receiving a sequence of incoming codes;

a comparator for comparing each of said incoming codes selectively with one of said first level code and second level code held in the store; and

a response controlling circuit for issuing a response when an incoming code matches the first level code or second level code held in the store.

8. A method of uniquely identifying one of a plurality of tags, each tag having a unique identification comprising a first level code and a second level code and means for issuing a response if an incoming code selectively matches one of said first level code and second level code, the method comprising:

issuing a first level code and awaiting any responses from tags, and, in the event that a response is received issuing a second level code and awaiting responses and, in the event that no response is received, issuing a next first level code and awaiting responses.

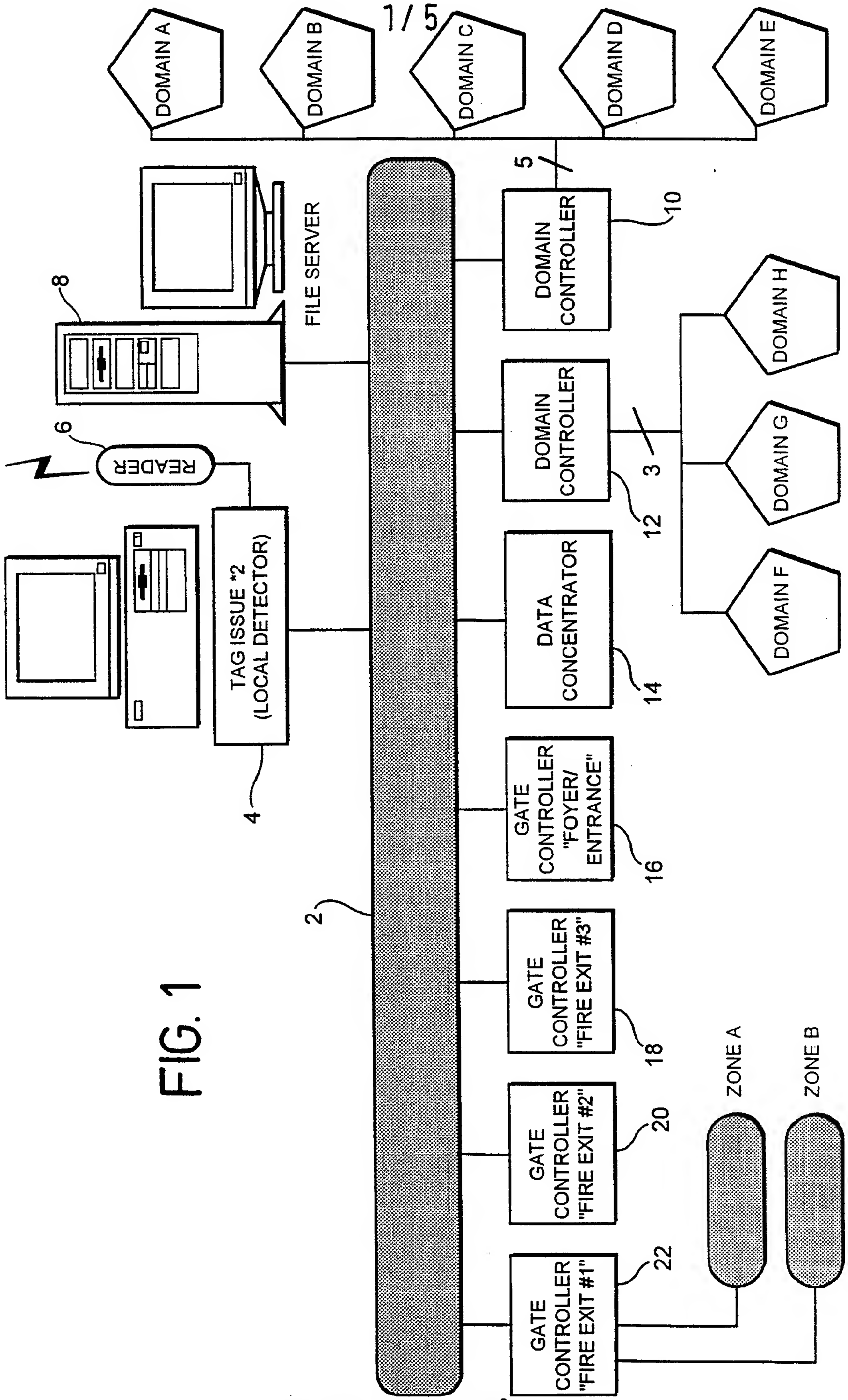

DOMAIN A
DOMAIN B
DOMAIN C
DOMAIN D
DOMAIN E
5
8
FILE SERVER
DOMAIN CONTROLLER
10
6
READER
DOMAIN CONTROLLER
3
12
DOMAIN H
DOMAIN G
DOMAIN F
TAG ISSUE *2 (LOCAL DETECTOR)
4
DATA CONCENTRATOR
14
GATE CONTROLLER "FOYER/ ENTRANCE"
16
2
GATE CONTROLLER "FIRE EXIT #3"
18
GATE CONTROLLER "FIRE EXIT #2"
20
GATE CONTROLLER "FIRE EXIT #1"
22
ZONE A
ZONE B

FIG. 1

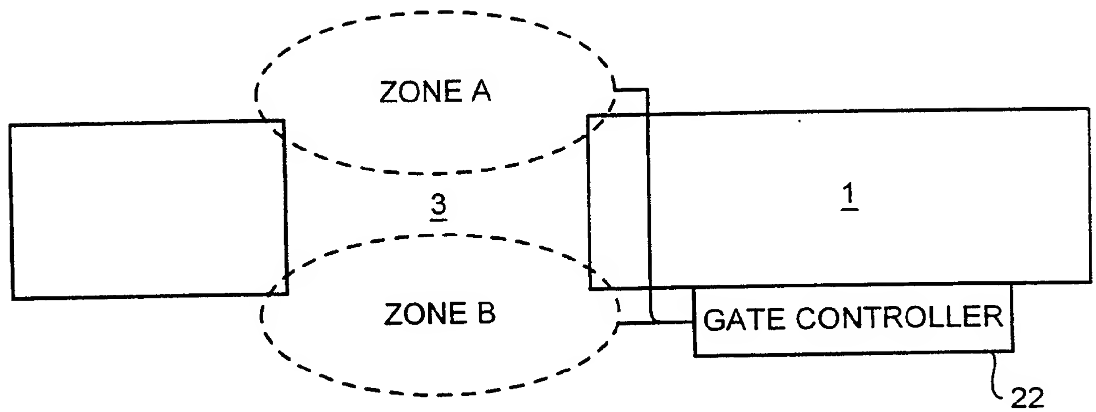

ZONE A
3
1
ZONE B
GATE CONTROLLER
22

FIG. 1a

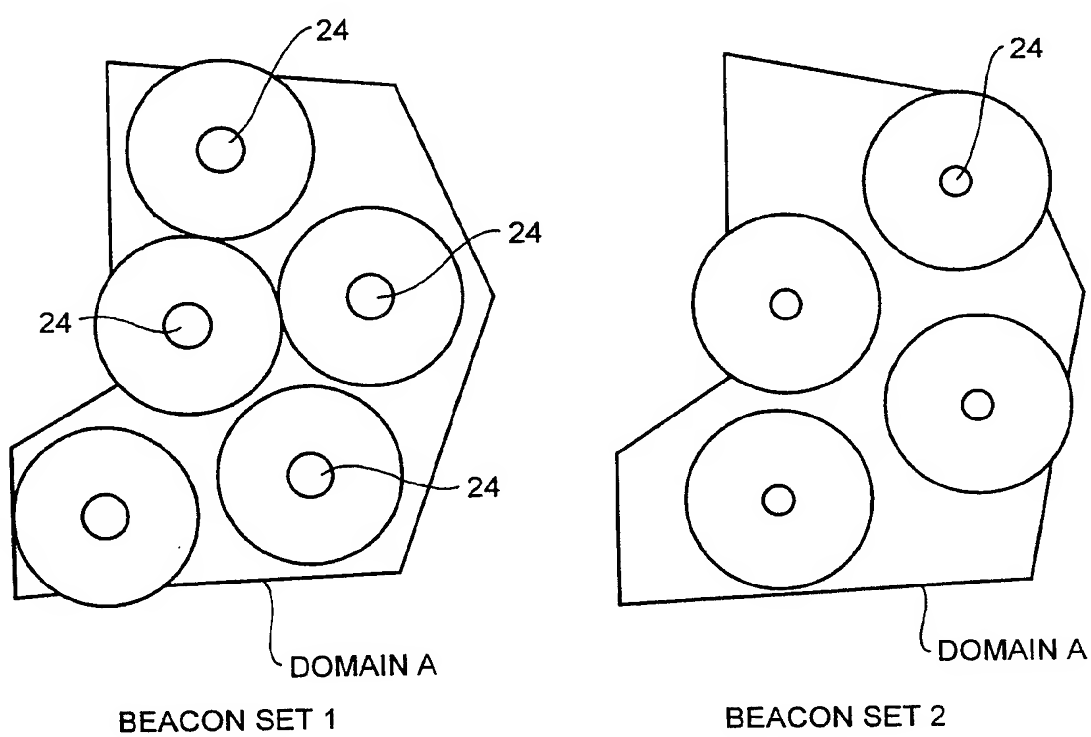

24
24
24
24
DOMAIN A
BEACON SET 1
24
DOMAIN A
BEACON SET 2

FIG. 2

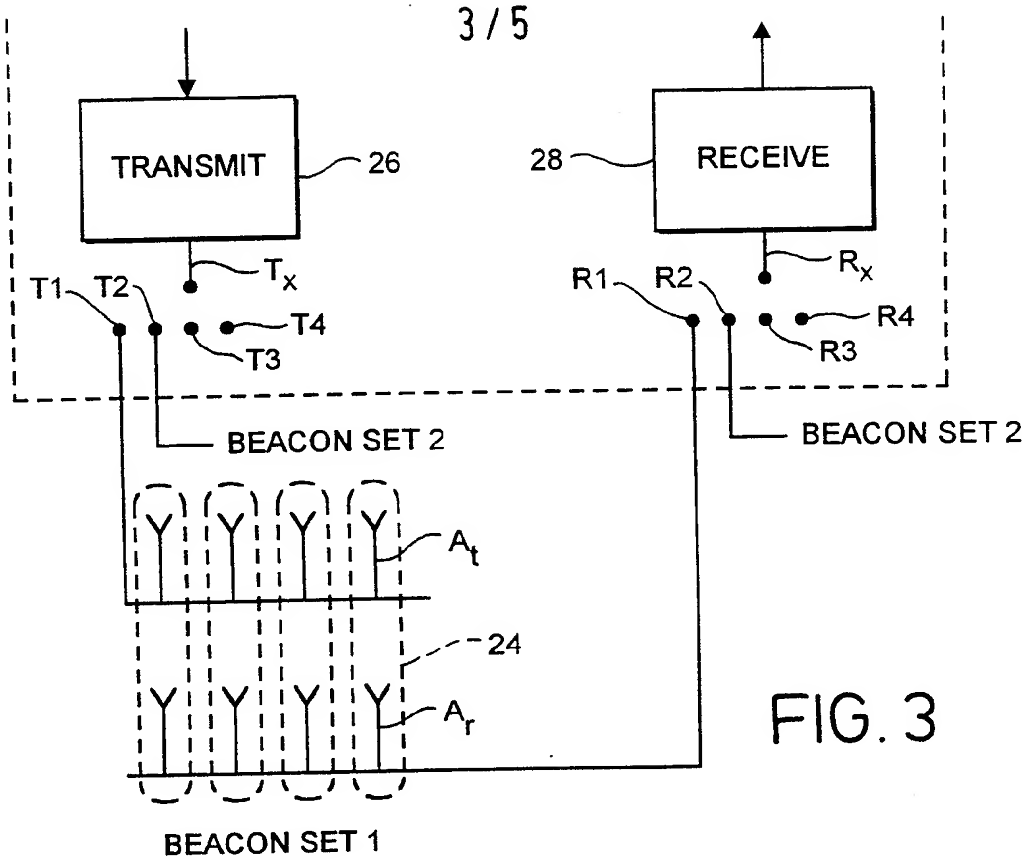

TRANSMIT
26
28
RECEIVE
Tx
Rx
T1
T2
T3
T4
R1
R2
R3
R4
BEACON SET 2
BEACON SET 2
At
24
Ar
BEACON SET 1

FIG. 3

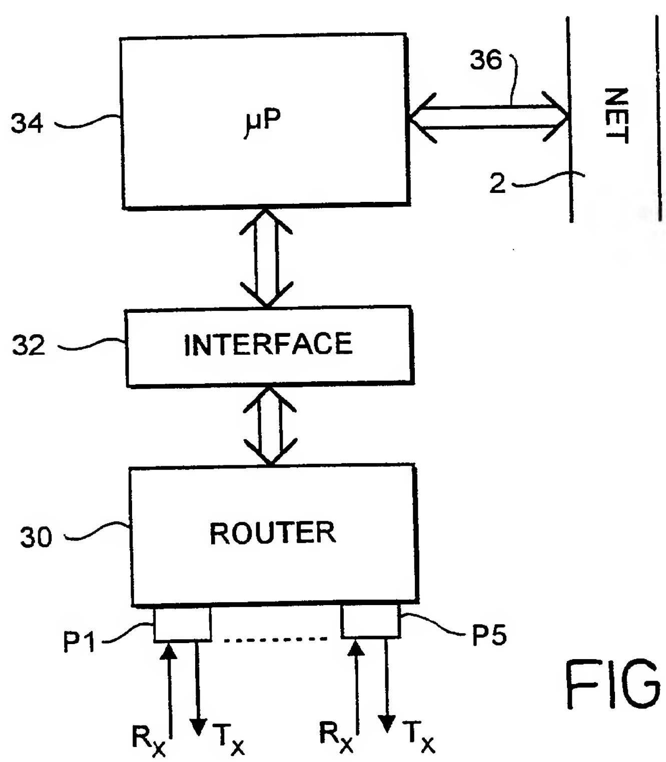
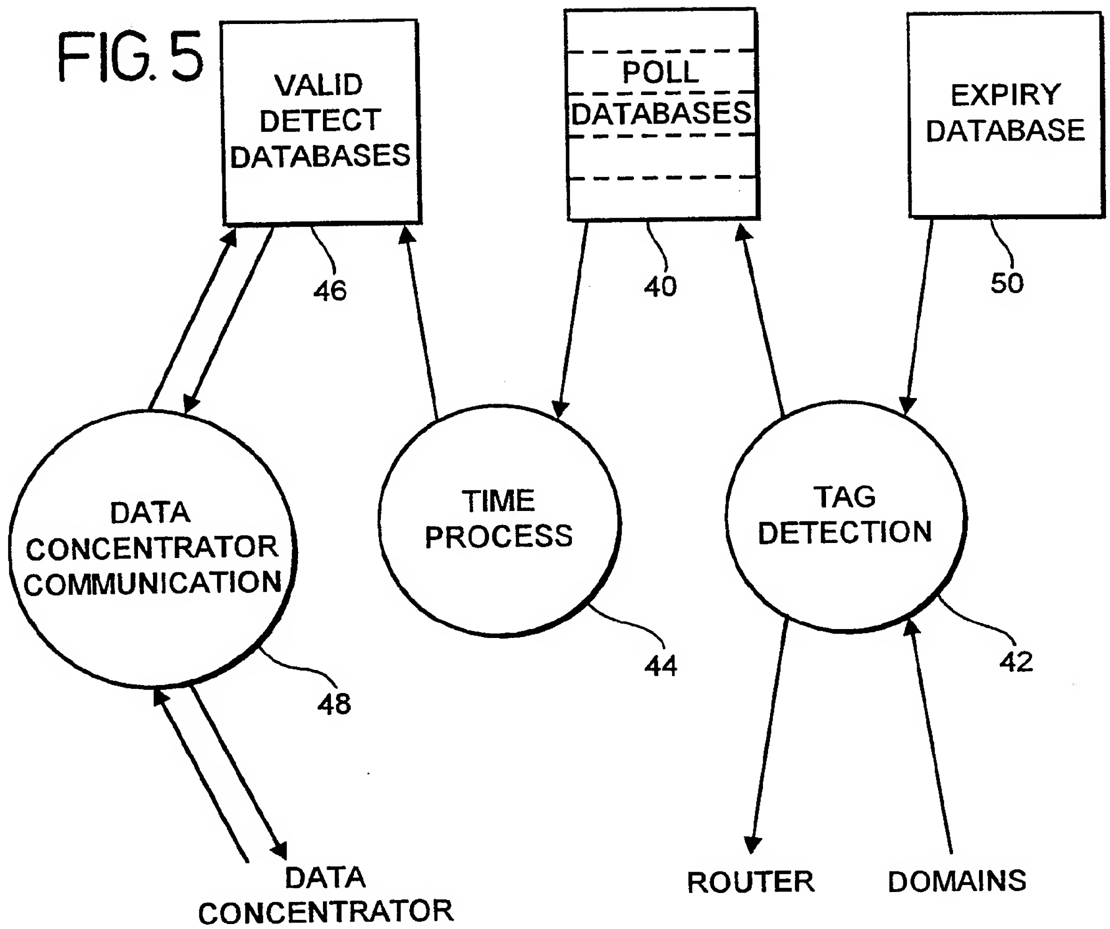

34
μP
36
NET
2
32
INTERFACE
30
ROUTER
P1
P5
Rx
Tx
Rx
Tx

FIG. 4

FIG. 5


VALID DETECT DATABASES
POLL DATABASES
EXPIRY DATABASE
46
40
50
DATA CONCENTRATOR COMMUNICATION
TIME PROCESS
TAG DETECTION
48
44
42
DATA CONCENTRATOR
ROUTER
DOMAINS

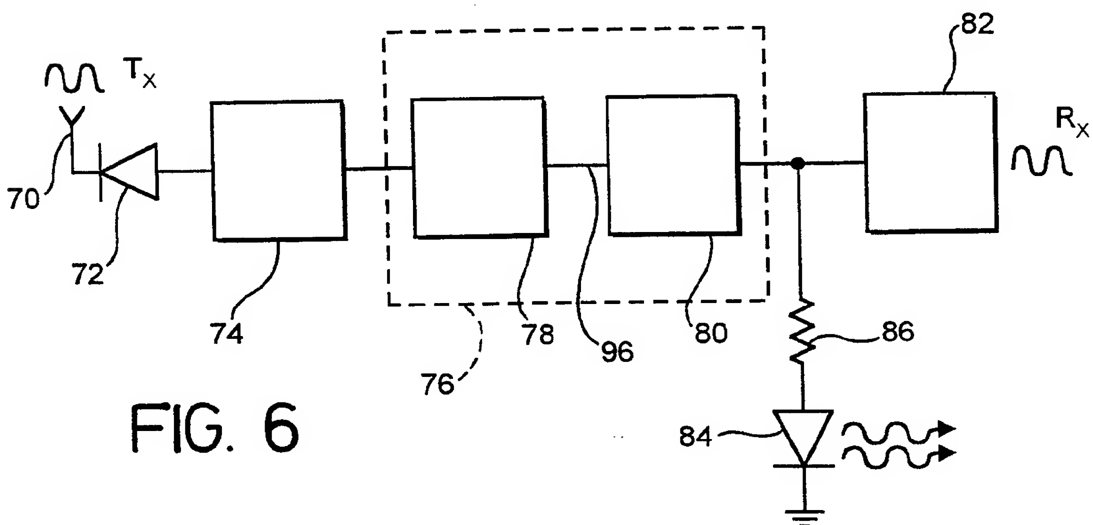

Tx
82
Rx
70
72
74
78
96
80
86
76
84

FIG. 6

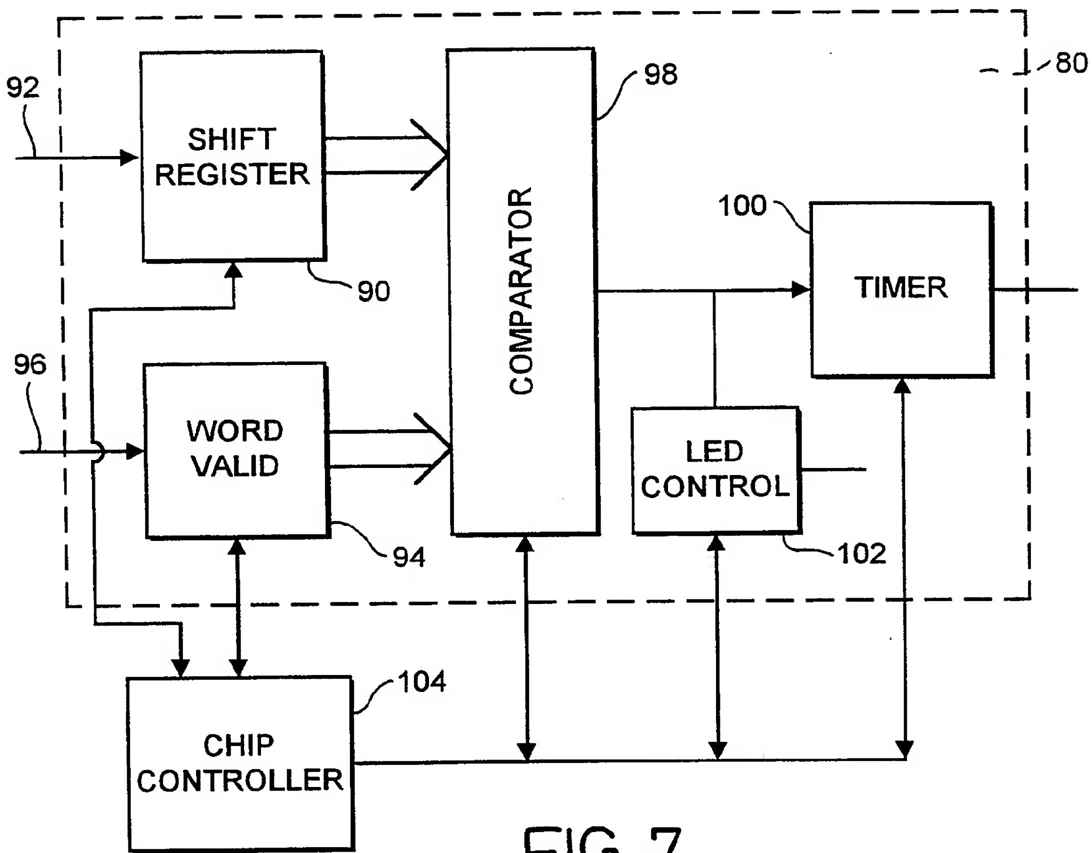


FIG.7

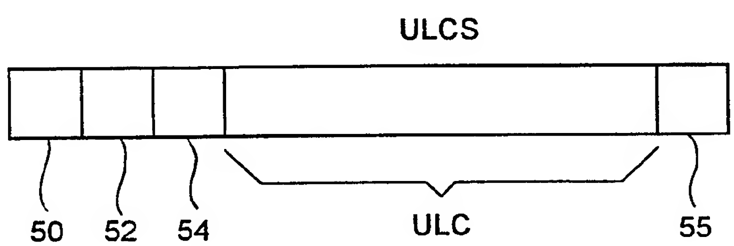


FIG.8

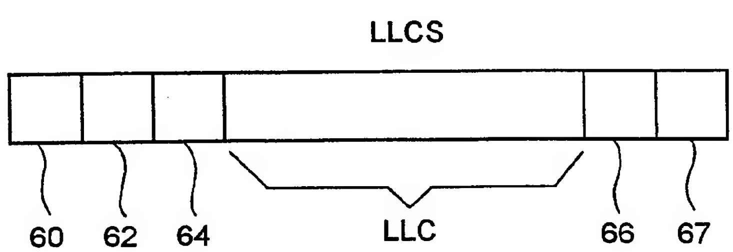


FIG.9

INTERNATIONAL SEARCH REPORT

International application No
PCT/GB 96/01535

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06K7/08 G06K7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP,A,0 285 419 (SATELLITE VIDEO SYSTEMS LTD) 5 October 1988	1-3,7,8
Y	see column 1, line 58 - column 2, line 47; claims	4
Y	EP,A,0 161 779 (SENELCO LTD) 21 November 1985 see page 2, line 16 - page 5, line 19	4
A		1,8
A	EP,A,0 494 114 (CSIR) 8 July 1992 see column 3, line 4 - column 5, line 30; figures	1,4,8
A	US,A,4 471 345 (BARRETT JR RAYMOND L) 11 September 1984 see column 2, line 33 - line 59; claims	1,8

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

1

Date of the actual completion of the international search	Date of mailing of the international search report
28 November 1996	09.12.96

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Gélébart, Y

INTERNATIONAL SEARCH REPORT

Internationa plication No
PCT/GB 96/01535

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP,A,0 322 701 (OMRON TATEISI ELECTRONICS CO) 5 July 1989 -----	

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/GB 96/01535

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
EP-A-0285419	05-10-88	CA-A-	1337946	16-01-96
		US-A-	5339073	16-08-94
		AT-T-	110480	15-09-94
		DE-D-	3851168	29-09-94
		DE-T-	3851168	30-03-95
		GB-A,B	2202981	05-10-88
EP-A-0161779	21-11-85	AU-B-	572321	05-05-88
		AU-A-	4533485	29-01-87
		GB-A,B	2157132	16-10-85
		JP-A-	62046281	28-02-87
		US-A-	4691202	01-09-87
EP-A-0494114	08-07-92	AU-B-	658857	04-05-95
		AU-A-	1000692	09-07-92
		CA-A-	2058692	05-07-92
		EP-A-	0685825	06-12-95
		JP-A-	4315081	06-11-92
		US-A-	5537105	16-07-96
US-A-4471345	11-09-84	AR-A-	231364	31-10-84
		BE-A-	895864	30-05-83
		CA-A-	1211522	16-09-86
		DE-A-	3305685	15-09-83
		FR-A-	2522829	09-09-83
		GB-A,B	2116808	28-09-83
		JP-C-	1640163	18-02-92
		JP-B-	3002271	14-01-91
		JP-A-	58162881	27-09-83
		NL-A-	8300643	03-10-83
		SE-B-	456278	19-09-88
		SE-A-	8301199	06-09-83
EP-A-0322701	05-07-89	JP-A-	1160233	23-06-89
		JP-A-	1162442	26-06-89
		AT-T-	140316	15-07-96
		DE-D-	3855417	14-08-96
		US-A-	5216419	01-06-93